



9111-14

## DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2018-0028]

### Privacy Act of 1974; System of Records

**AGENCY:** Department of Homeland Security.

**ACTION:** Notice of a New System of Records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, “Department of Homeland Security/U.S. Customs and Border Protection-025 National Frontline Recruitment and Hiring System of Records.” This system of records allows the DHS/U.S. Customs and Border Protection (CBP) to collect and maintain records on individuals for the purpose of marketing information related to CBP employment, managing communication with potential applicants or individuals who attend career fairs or meetings at which CBP maintains a presence for recruitment and hiring, and for other recruitment and hiring activities for which mailing or contact lists may be created. This newly established system will be included in DHS’s inventory of record systems.

**DATES:** Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This new system will be effective upon publication. Routine uses will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

**ADDRESSES:** You may submit comments, identified by docket number DHS-2018-0028 by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Philip S. Kaplan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

*Instructions:* All submissions received must include the agency name and docket number DHS-2018-0028. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

*Docket:* For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For general questions, please contact: Debra L. Danisek, Privacy Officer, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue NW, Washington, D.C. 20029 or [Privacy.CBP@cbp.dhs.gov](mailto:Privacy.CBP@cbp.dhs.gov), (202) 344-1610. For privacy questions, please contact: Philip S. Kaplan, (202) 343-1717, [Privacy@hq.dhs.gov](mailto:Privacy@hq.dhs.gov), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

## **SUPPLEMENTARY INFORMATION:**

### **I. Background**

Recruiting and retaining a world-class law enforcement workforce is one of CBP's top mission support priorities. To generate a sufficient number of qualified applicants for critical frontline law enforcement positions, CBP must cultivate a large volume of interested and well-qualified applicants. CBP uses recruitment outreach, market research, data analytics, advertising, and marketing services to conduct recruiting

and hiring campaigns to meet staffing requirements. These targeted efforts identify potential applicants and help them navigate the complex and multi-step hiring process for CBP frontline officers and agents. To meet aggressive recruiting goals, CBP frontline recruitment strategy requires data analytics, targeted marketing and recruiting, technology innovations, call center support, additional specialized skillsets, and internal process improvements.

On January 25, 2017, the President issued the Executive Order 13767, and provided direction to CBP to take appropriate action to recruit and hire individuals for critical frontline law enforcement positions (such as U.S. Border Patrol Agents, Air and Marine Interdiction Agents, and CBP Officers).

CBP conducts coordinated initiatives in support of frontline recruitment and hiring, including: (1) marketing, branding, and public opinion research; (2) direct advertising to individuals who have expressed an interest in employment opportunities with CBP; (3) direct advertising to individuals who have expressed an interest in employment opportunities to a third-party for employment purposes, who have affirmed that they may be contacted by potential employers; and (4) communication with individuals who have provided their information to CBP, including response to screening questions, in support of the preliminary application process. These activities might entail the collection of limited biographic information, contact information, and information pertinent to employment from members of the public who have not yet applied for a CBP job announcement. In addition, CBP may use aggregated data analytics and enhanced advertisements to locate potential recruits in support of efforts to maintain congressionally-mandated CBP staffing levels.

This SORN provides coverage for CBP's recruitment and hiring efforts for frontline positions. The SORN does not cover records associated with the formal hiring process once a potential applicant submits an application for employment. The Office of Personnel Management (OPM) is responsible for all hiring activities for employment with Federal agencies. For these activities, the relevant OPM SORNs continue to apply.

Consistent with DHS's information sharing mission, information stored in the DHS/CBP-025 National Frontline Recruitment and Hiring System of Records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/CBP may share information with appropriate Federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

This newly established system will be included in DHS's inventory of record systems.

## II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial

Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/CBP-025 National Frontline Recruitment and Hiring System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

**SYSTEM NAME AND NUMBER:** Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-025 National Frontline Recruitment and Hiring System of Records.

**SECURITY CLASSIFICATION:** Unclassified.

**SYSTEM LOCATION:** DHS/CBP maintains records at its Headquarters at 1300 Pennsylvania Avenue NW, Washington, D.C. 20229, and in field offices, and contractor-owned and operated facilities. DHS/CBP stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media and will be maintained within a DHS web portal.

**SYSTEM MANAGER(S):** Executive Assistant Commissioner, Enterprise Services, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue NW, Washington, D.C. 20029.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

5 U.S.C. 302, Delegation of authority; 44 U.S.C. 3101, Records management by agency heads, general duties; Executive Order 13767, Border Security and Immigration Enforcement Improvements (January 25, 2017).

**PURPOSE(S) OF THE SYSTEM:** The purpose of this system is to conduct recruitment, marketing, outreach, and advertising to potential candidates for CBP frontline law enforcement positions; generate leads and maintain lists of potential applicants for recruiting purposes based on commercially available demographic or subscription lists or from community, civic, educational institutions, military, and other sources; identify quality leads based on pre-screening question responses; manage all tracking and communications with potential leads and conduct outreach to retain applicants during the hiring process; maintain logs and respond to applicant questions from a national call center; reengage withdrawn applicants for frontline hiring positions and invite them to reapply to CBP opportunities; and conduct data analytics for recruitment strategies, to measure the effectiveness of outreach campaigns. CBP will maintain aggregated, non-personally identifiable web data analytics to measure the success of online marketing and advertising initiatives. CBP invites candidates to voluntarily self-identify for purposes of the DHS equal employment opportunity program to include those policies, practices, and procedures to ensure that all qualified individuals and potential applicants receive an equal opportunity for recruitment, selection, advancement, and every other term and privilege associated with CBP employment opportunities.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Potential applicants for critical CBP frontline law enforcement positions (U.S. Border Patrol

Agents, Air and Marine Interdiction Agents, and CBP Officers) covered by the system include:

1. Individuals who express interest in a frontline law enforcement position and voluntarily provide information to CBP.
2. Individuals who withdraw from the hiring process for frontline law enforcement positions.
3. Individuals who receive targeted marketing information from CBP to apply for a CBP frontline law enforcement position based on commercially available mailing lists (e.g., particular magazine or cable channel subscribers) or from community, civic, educational institutions, military, and other sources.

#### **CATEGORIES OF RECORDS IN THE SYSTEM:**

CBP maintains various types of information related to recruiting and outreach records for national frontline positions, including:

- First and last name;
- Age or date of birth;
- Gender;
- Phone numbers;
- Email addresses;
- Mailing addresses, including ZIP code;
- Military status (e.g., veteran, active duty);
- Other biographic and contact information voluntarily provided to DHS by individuals covered by this system of records solely for recruitment and hiring activities;

- Computer-generated identifier or case number when created in order to retrieve information;
- Status of opt-in/consent to receive targeted marketing and advertising based on the individual's expressed area of interest in CBP employment opportunities; and
- Responses to pre-screening questions, including information related to: (1) an individual's possession of, or eligibility to, carry a valid driver's license (yes or no response only); (2) any reason why the individual may not be able to carry a firearm (yes or no response only); (3) interest level in CBP employment; (4) U.S. residency information (limited to length of residency only); and (5) any additional information in support of preliminary hiring activities.

**RECORD SOURCE CATEGORIES:** CBP may obtain the records about potential applicants in this system either directly from the individual, from a third-party with whom the individual has granted permission to share his or her information with potential employers, or from community, civic, educational institutions, military, and other sources. CBP will obtain records about withdrawn applicants from existing internal CBP human resources systems.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING**

**CATEGORIES OF USERS AND PURPOSES OF SUCH USES:** In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including U.S. Attorneys Offices, or other Federal agency conducting litigation or proceedings before any court, adjudicative, or



administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee or former employee of DHS in his/her official capacity;
3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. sec. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate Federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** DHS/CBP stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** DHS/CBP retrieves records by an individual's name.

## **POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF**

**RECORDS:** In accordance with General Records Schedule (GRS) 6.5, Item 20, and GRS 5.2, Item 20, DHS/CBP will delete records when superseded, obsolete, or when an individual submits a request to the agency to remove the records. In general and unless it receives a request for removal, CBP will maintain these records for 5 years, after which point they will be considered obsolete and no longer necessary for CBP operations.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** DHS/CBP safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. CBP has imposed strict controls to minimize the risk of compromising the information that is being stored.

Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**RECORD ACCESS PROCEDURES:** Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and DHS/CBP's FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "Contacts Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about the individual may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, <http://www.dhs.gov/foia> or 1-866-431-0486. In addition, the individual should:

- Explain why he/she believe the Department would have information on him/her;
- Identify which component(s) of the Department the individual believes may have the information about him/her;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from the second individual certifying his/her agreement for the first individual to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

**CONTESTING RECORD PROCEDURES:** For records covered by the Privacy Act or covered JRA records, see “Record Access Procedures” above.

**NOTIFICATION PROCEDURES:** See “Record Access Procedures.”

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** None.

**HISTORY:** None.

Philip S. Kaplan,  
Chief Privacy Officer,  
Department of Homeland Security.  
[FR Doc. 2018-12416 Filed: 6/8/2018 8:45 am; Publication Date: 6/11/2018]